I_0:

25	4	27	41	20
42	31	33	38	17
21	5	1	19	34
36	16	18	40	10
0	23	11	26	44
22	9	37	12	35
43	3	15	7	30
8	32	24	14	29
2	28	6	39	13

I_1:

42	43	7	1	6
27	23	10	29	13
26	15	38	19	40
12	37	9	32	36
14	25	22	33	28
8	41	4	30	5
16	0	35	11	3
34	20	2	18	31
44	21	24	17	39

F:

4	42	33	27	20	25	31	41
17	19	34	21	38	5	1	10
0	18	26	36	23	16	40	44
9	3	12	35	37	43	11	22
29	14	7	8	30	24	32	15
6			28	39	13		2

G_0:

(0,5)	(0,0)	(0,3)	(0,7)	(0,4)
(0,1)	(0,6)	(0,2)	(1,4)	(1,0)
(1,3)	(1,5)	(1,6)	(1,1)	(1,2)
(2,3)	(2,5)	(2,1)	(2,6)	(1,7)
(2,0)	(2,4)	(3,6)	(2,2)	(2,7)
(3,7)	(3,0)	(3,4)	(3,2)	(3,3)
(3,5)	(3,1)	(4,7)	(4,2)	(4,4)
(4,3)	(4,6)	(4,5)	(4,1)	(4,0)
(5,7)	(5,3)	(5,0)	(5,4)	(5,5)

G_1:

(0,1)	(3,5)	(4,2)	(1,6)	(5,0)
(0,3)	(2,4)	(1,7)	(4,0)	(5,5)
(2,2)	(4,7)	(1,4)	(1,1)	(2,6)
(3,2)	(3,4)	(3,0)	(4,6)	(2,3)
(4,1)	(0,5)	(3,7)	(0,2)	(5,3)
(4,3)	(0,7)	(0,0)	(4,4)	(1,5)
(2,5)	(2,0)	(3,3)	(3,6)	(3,1)
(1,2)	(0,4)	(5,7)	(2,1)	(0,6)
(2,7)	(1,3)	(4,5)	(1,0)	(5,4)

FIG. 1

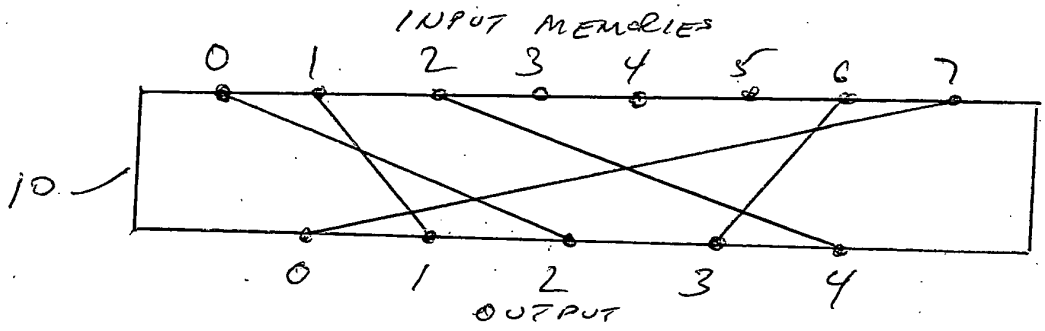

FIG. 2

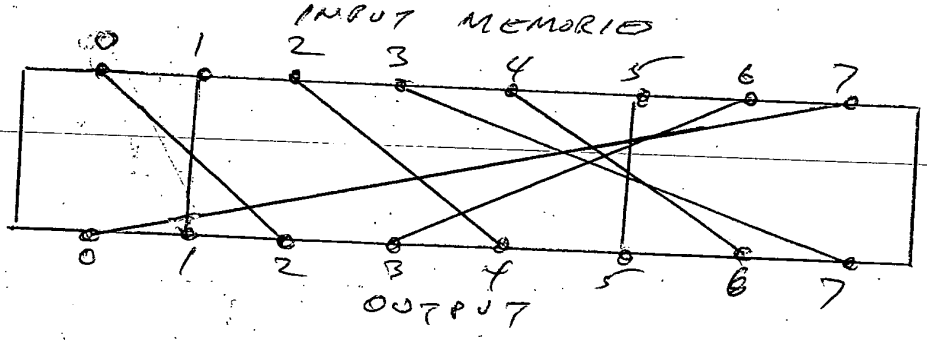

FIG. 3

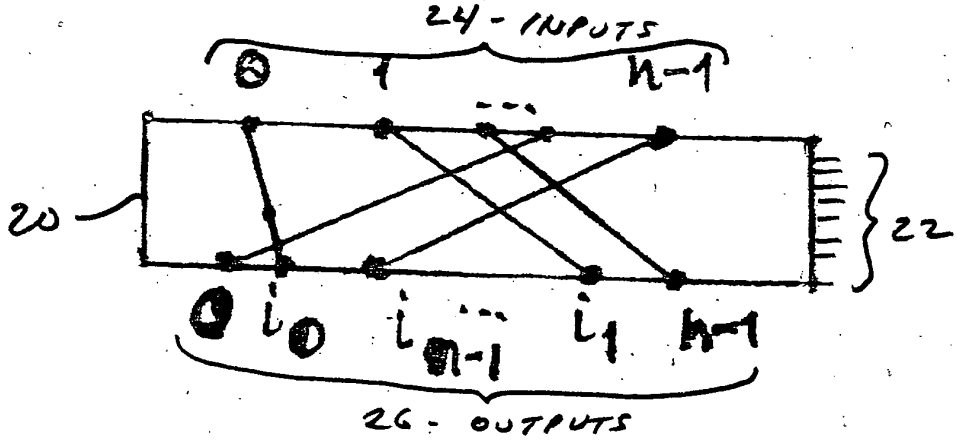

FIG. 4

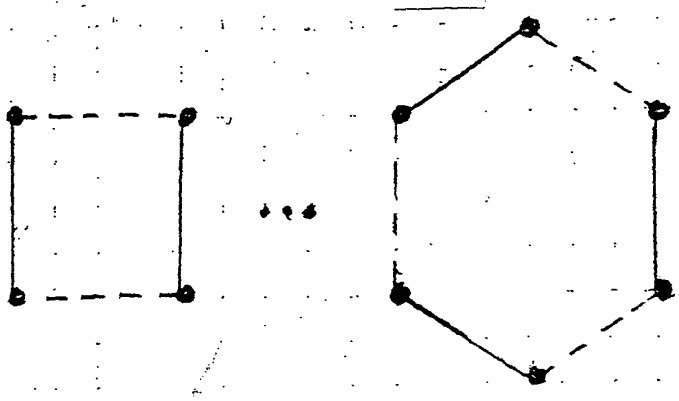

FIG 5. Graph G

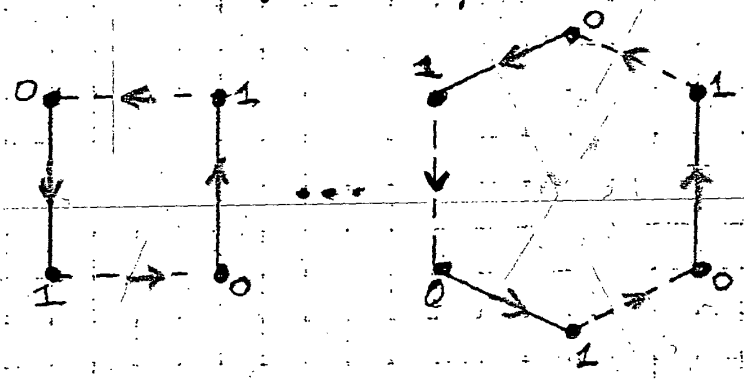

FIG 6. Coloring of vertices

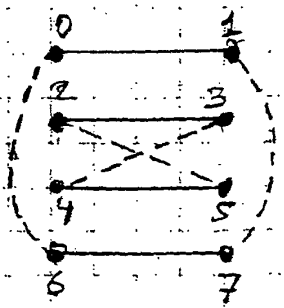

FIG 7 Graph G of permutation P=(7,1,0,6,2,5,3,4)

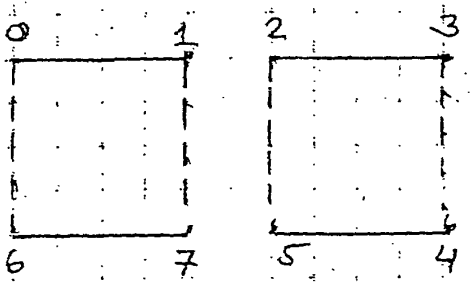

FIG 8. Cycles of G

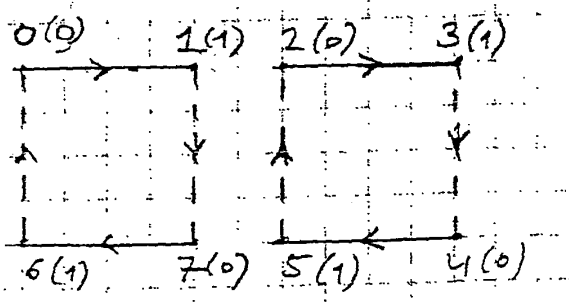

FIG 9 Coloring of G vertices

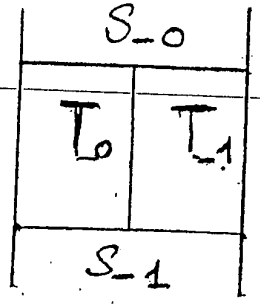

FIG. 10 Table T

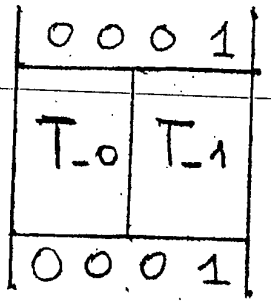

FIG. 11. T for P

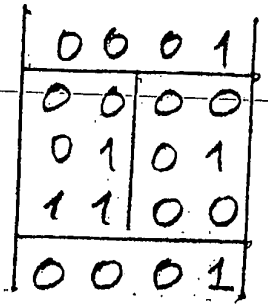

FIG. 12. T for P

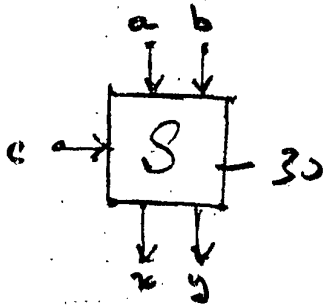

FIG. 14

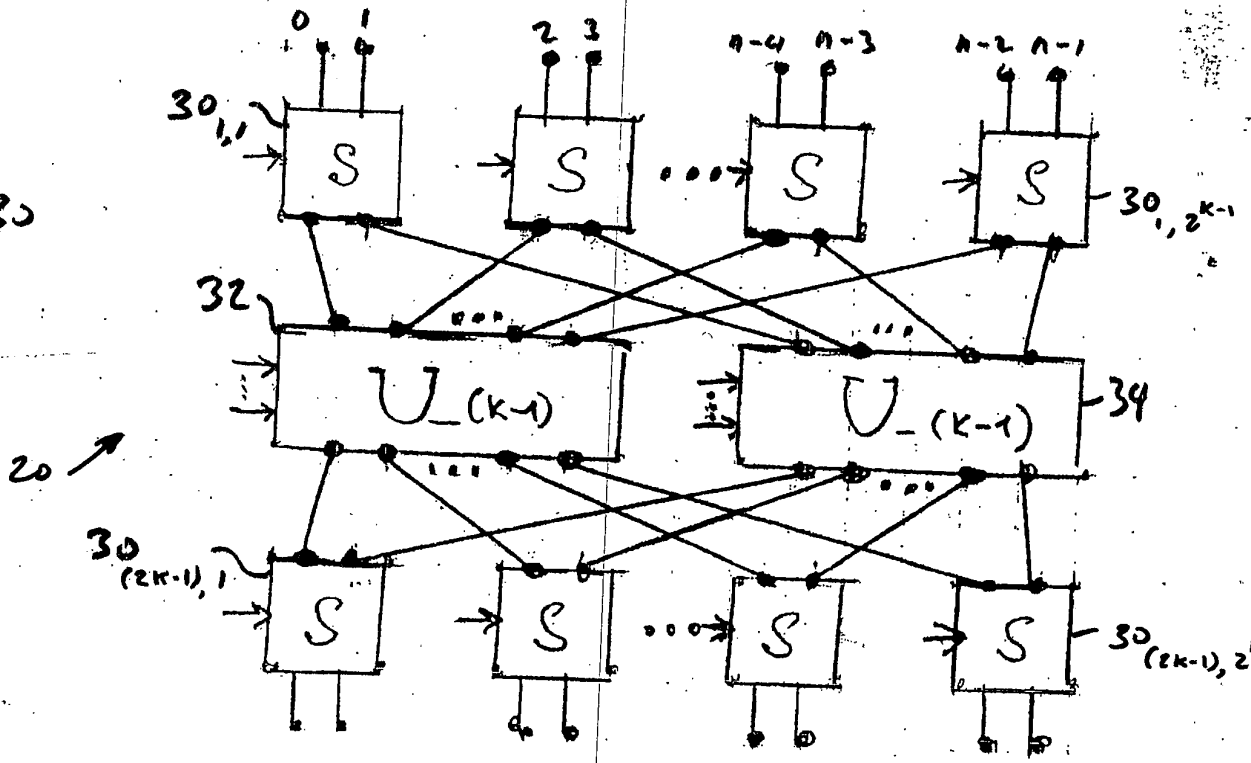

FIG. 15

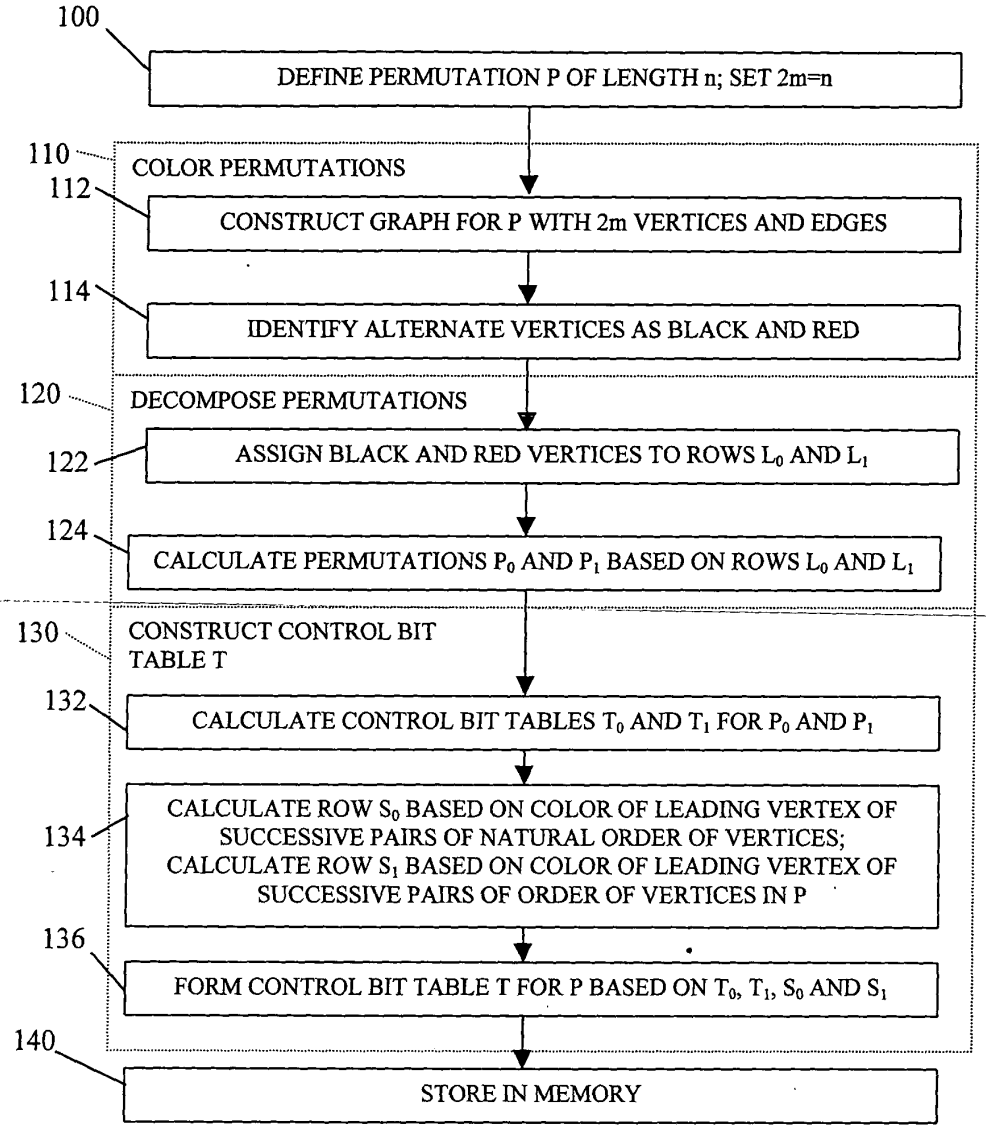
100
DEFINE PERMUTATION P OF LENGTH n; SET 2m=n
110
COLOR PERMUTATIONS
112
CONSTRUCT GRAPH FOR P WITH 2m VERTICES AND EDGES
114
IDENTIFY ALTERNATE VERTICES AS BLACK AND RED
120
DECOMPOSE PERMUTATIONS
122
ASSIGN BLACK AND RED VERTICES TO ROWS L_0 AND L_1
124
CALCULATE PERMUTATIONS P_0 AND P_1 BASED ON ROWS L_0 AND L_1
130
CONSTRUCT CONTROL BIT TABLE T
132
CALCULATE CONTROL BIT TABLES T_0 AND T_1 FOR P_0 AND P_1
134
CALCULATE ROW S_0 BASED ON COLOR OF LEADING VERTEX OF SUCCESSIVE PAIRS OF NATURAL ORDER OF VERTICES; CALCULATE ROW S_1 BASED ON COLOR OF LEADING VERTEX OF SUCCESSIVE PAIRS OF ORDER OF VERTICES IN P
136
FORM CONTROL BIT TABLE T FOR P BASED ON T_0, T_1, S_0 AND S_1
140
STORE IN MEMORY

FIG. 13

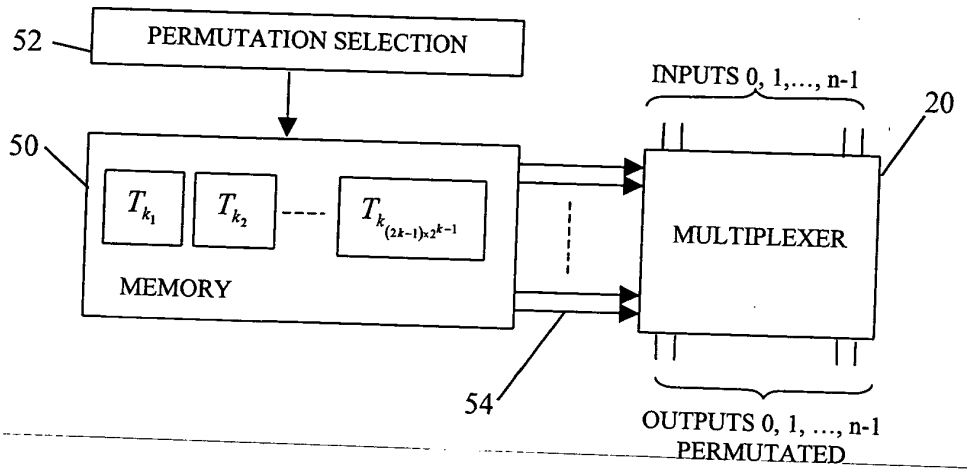
52
PERMUTATION SELECTION
INPUTS 0, 1,..., n-1
20
50
T_{k_1}
T_{k_2}
$T_{k_{(2k-1)\times 2^{k-1}}}$
MEMORY
MULTIPLEXER
54
OUTPUTS 0, 1, ..., n-1
PERMUTATED

FIG. 16